20XX-01-XXXX

Onboard Cybersecurity Diagnostic System for Connected Vehicles

Author, co-author (Do NOT enter this information. It will be pulled from participant tab in MyTechZone)

Affiliation (Do NOT enter this information. It will be pulled from participant tab in MyTechZone)

Abstract

Today's advanced vehicles contain numerous sensors and exhibit a high degree of interactions among vehicle's components (e.g., sensors, devices, systems, systems- of-systems) across sensing, communication, and control layers. While driving on the road, hackers only need to be within communication range of the vehicle to attack it. In this article, we discuss the On-Board Diagnostic (OBD) new regulations , OBD system vulnerabilities and the latest vehicle cyber security threats that include malware attacks. We propose three cybersecurity attack detection and defense methods: Cyber-Attack detection algorithm, Time-Based CAN Intrusion Detection Method and, Feistel Cipher Block Method. These control methods autonomously diagnose a cybersecurity problem in a vehicle's onboard system using an OBD interface, such as OBD-II when a fault caused by a cyberattack is detected, All of this is achieved in an communication structure where the vehicle sensors and onboard ECUs are connected with each other via an internal network. The results discussed here focus on the first detection method that is Cyber-Attack detection algorithm.

Index Terms—hybrid electric vehicle, onboard diagnostic, autonomous connected vehicle, cybersecurity, control algorithm, battery electric vehicle

Introduction

Until recently, vehicles have been isolated from the internet. The only exception was the interface for vehicle diagnostics with OBD-II port being a wired interface, OBD-II port could rely on the physical protection offered by the vehicle's chassis, like the electronic control units (ECUs) and the in-vehicle network (IVN). But things are changing rapidly. Most modern vehicles already allow smartphones to be paired via Bluetooth with the car's entertainment system for hands-free phone calls or to play music. And it doesn't stop there. Many modern vehicles are wirelessly connected to the internet which not only enables additional services in the car but also provide remote control over the vehicle such as remote unlocking and starting. To improve safety, these cars will furthermore be equipped with eCall and V2X communication technologies, complemented by ADAS systems that offer advanced driving assistance features and ultimately, autonomous driving.

These days, autonomous vehicles (AV) driving without the intervention of a driver use onboard software applications to identify driving conditions. AVs now have the ability to diagnose and check for any hazard causing events using various kinds of sensors installed in the vehicle. These complex diagnostic functions are achieved with Electronic Control Units (ECUs), ECU's play a critical role in today's vehicle and hence its rationality along with complex sensors, actuators and onboard system software ought to be ensured in order to protect for vehicle safety.

A handful of extensively advertised attacks has demonstrated vulnerability, consisting of a 2014 occurrence entailing an OEM. Hackers looking to expose possible vulnerabilities found a password to a Wi-Fi hot spot as well as cellular connections made use of vehicle's main screen and entertainment system. From there, they accessed the vehicle's interior computer network and also took control of functions ranging from the door locks and also window wipers to electronically assisted steering. This event recalled 1.4 million vehicles and worked as a cautioning to the market that vehicle networks are no longer islands unto themselves.

From the regulation's perspective, government agencies have started to address cybersecurity threats by establishing regulations that are not specific to AVs, conducting further research right into cybersecurity dangers for AVs and all vehicles in general, as well as giving standards. Some federal governments such as that of the UK and also Singapore have actually additionally started informing the general public of cybersecurity threats, whereas the federal governments of Japan and also South Korea have yet to suggest their intents to attend to cybersecurity risks. In the US, the federal government has actually taken actions to explore vehicle cybersecurity risks and has made recommendations to handle AV-specific cybersecurity threats. In 2012, the National Highway Web Traffic Safety And Security Management (NHTSA) [1] set up a new department to research "safety and security, security, and reliability of facility, adjoined, electronic vehicle systems" as well as has set up an Electronic devices Council to enhance partnership throughout the entire NHTSA organization concerning automobile electronic devices and cybersecurity .

The current OBD regulations in U.S. requirements [2] enforced by California Air Resources Board (CARB) do not cover zero emission vehicles (ZEV), such as battery electric vehicles (BEV). With the quick innovations in battery modern technologies, such as raised power density, improved reliability, reduced degradation, and improved battery management systems, as well as enhances in motor modern technology performance recently, BEVs are now strong competitors for vehicles with traditional powertrain systems among consumers without extended driving needs and are expected to expand in market shares in the coming years. With an upward trend of even more consumers driving BEVs, it is reasonable to predict a gain from industry standardization for the tracking and reporting requirements for BEV electrical propulsion systems. In addition, some lawmakers [2] have actually already begun to make proposals to mandate monitoring and also reporting requirements on the on-board systems in BEVs.

corresponding cybersecurity DTC is set and stored in the memory once the attack is confirmed and also a notification is sent to the customer on the vehicle dashboard of a possible Cyber-Attack on the vehicle .

Cyber-Attack detection algorithm solution on the CAN bus is only viable if it addresses the following constraints:

- No change in the CAN-bus protocol (i.e., change to message headers or additional messages)
- Restrict the number of times an attacker can attempt to send a forged message, as well as the number of authenticated messages that the attacker can view (while attempting the forgery)
- Zero overhead
- Minimal performance impact
- Allow recovery after reboot (of receiver and senders)

The method 1 algorithm that is Cyber-Attack detection algorithm has to be further evaluated for the following above constrains and compared with the other methods such as Time-Based CAN Intrusion Detection Method and Feistel Cipher block method which will be discussed in future works.

Summary/Conclusions

In this paper, a novel Cyber-Attack detection method and a fault-tolerant operation control algorithm solution are proposed for Simple Spoofing Attack. The fault detection method is simple for implementation and it can locate the faulty ECU by analyzing CAN data , CAN_ID and the vehicle drive state. The fault-tolerant capability has been achieved by analyzing the characteristics of the CAN signals . The robustness of the detection can be further improved by adding a second layer of check where in the second-step detection rule includes a rule for detecting a sign of an abnormality assumed to be an attack by performing state transition analysis or time-series (sequence pattern) analysis using a series of received electronic control commands (CAN IDs) as discussed in the time based CAN intrusion detection methods. The performance of the time-based methods and Feistel Cipher block method with improved deep learning models can improve the use case and efficiency of the detection. These methods and its algorithm performance results will be further discussed in future works.

References

1. NHTSA . *Nhtsa and Vehicle Cybersecurity*; National Highway Traffic Safety Administration :Washington,DC,USA,2018.
2. CARB. *California Air Resource Board OBD regulations*, www.arb.ca.gov
3. S. Baek, J. Jang, Implementation of Integrated OBD-II Connector with External Network, Science Direct Journal, 2014.
4. Kavian Khorsravinia, et. Al., *Integrated OBD-II and mobile application for electric vehicle (EV) monitoring system*, IEEE end International Conference on Automatic Control and Intelligent Systems, 2017
5. Lindsey Heineman, Andrew Zettel, *ZERO EMISSIONS VEHICLES (ZEV'S) AND OBD*, SAE On-board Diagnostics Symposium Americas, Garden Grove, CA, USA, 2019
6. Andrew Zettel, *EV Roundtable Discussions*, SAE On-board Diagnostics Symposium Digital Summit, Online Virtual Event, 2020.
7. D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: vehicle virus," *in Proc. Int. Conf. on Communication Systems and Networks,* Langkawi, Malaysia, 2008, pp. 66-72.
8. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham,S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Security*, San Francisco, CA, 2011.
9. W. Yan, "A Two-year Survey on Security Challenges in Automotive Threat Landscape," in *Proc. IEEE ICCVE*, Shenzhen Oct. 2015, pp. 185-189.
10. T. Zhang, H. Antunes and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things*, vol. 1, no. 1, Feb 2014, pp. 10-21.
11. Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. CCS*, 2015, pp. 1004–1015, doi: 10.1145/2810103.2813679.
12. L. Ljung. System Identification: Theory for the User. Pearson Education, 1998
13. YongBin Zhou, DengGuo Feng, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing,"in International Association for Cryptologic Research,2005, https://eprint.iacr.org/2005/388
14. Timo van Roermund ,Andreas Bening , NXP automotive business unit , "Cybersecurity for ECUs:Attacks and Countermeasures,"[online].Available: https://www.nxp.com/docs/en/white-paper/Cybersecurity-ECUs-WP.pdf
15. M. Farhadi and M. Abapour, "Three-switch three-phase inverter with improved dc voltage utilization," *IEEE Transactions on Industrial Elec-tronics*, vol. 66, no. 1, pp. 14–24, 2018.
16. Z.-Z. Elektrotechnik-und, "Handbook for robustness validation of auto-motive electrical/electronic modules."
17. S. Nathan, "Hackers after your car? Tackling automotive cyber security," The Engineer, Sept. 24, 2015. [Online]. Available: https://www.theengineer.co.uk/hackers-after-your-car-tackling-automotive-cyber-security/ [Accessed 2016 03 21]
18. S. Khandelwal, "Car Hackers Could Face Life In Prison. That's Insane!," The Hacker News, May 01, 2016. [Online]. Available: http://thehackernews.com/2016/05/car-hacker-prison.html [Accessed 2016 05 23]
19. A. Greenberg, "Hackers remotely kill a Jeep on the highway – with me in it," WIRED, July 21, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed 2015 09 30].
20. D. Lodge, "Hacking the Mitsubishi Outlander PHEV hybrid," PenTestPartners, June 05, 2016. [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ [Accessed 2016 08 14].
21. FD. Garcia, D. Oswald, T. Kasper and P. Pavlidès, "Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems," in *Proc. 25th USENIX Security*, Austin, TX, 2016.
22. R. Hull, "Nissan disables Leaf electric car app after revelation that hackers can switch on the heater to drain the battery," Thisismoney,Feb. 26, 2016.[Online].Available: http://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html [Accessed 2016 06 27].
23. R. Link, "Is Your Car Broadcasting Too Much Information?," Trend Micro Inc., July 28, 2015. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/?_ga=1.215918871.1268134788.1466680640 [Accessed 2016 06 27].
24. S. Curtis, "Self-driving cars can be hacked using a laser pointer," The Telegraph, Sept. 08, 2015. [Online]. Available: http://www.telegraph.co.uk/technology/news/11850373/Self-

driving-cars-can-be-hacked-using-a-laser-pointer.html [Accessed 2016 06 25].

25. TU-Automotive Ltd, TU-Automotive Cyber Security Europe, 2-3 November 2016, ICM - Internationales Congress Center München, Germany. [Online]. Available: http://www.tu-auto.com/cyber- security-europe/ [Accessed 2016 06 25].
26. I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in Proc. IEEE DSN-W, Budapest, June 2013, pp. 1-12.
27. D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: vehicle virus," in *Proc. Int. Conf. on Communication Systems and Networks*, Langkawi, Malaysia, 2008, pp. 66-72.
28. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham,S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in Proc. 20th USENIX Security, San Francisco, CA, 2011.
29. W. Yan, "A Two-year Survey on Security Challenges in Automotive Threat Landscape," in *Proc. IEEE ICCVE*, Shenzhen Oct. 2015, pp. 185-189.
30. N. Lyamin, A. Vinel, M. Jonsson and J. Loo, "Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks," *IEEE Commu. Letters*, vol. 18, no. 1, pp. 110-113, Jan. 2014.
31. Ericsson, "Connected Vehicle Cloud Under the Hood," Ericsson, 2015. [Online].Available: http://archive.ericsson.net/service/internet/picov/get?DocNo=28 7 01-FGD101192 [Accessed 2016 04 18]
32. National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," Report No. DOT HS 812 333, Washington, DC,Oct2016.[Online]. Available:https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityF orModernVehicles.pdf [Accessed 2017 01 10]
33. Sumanth Dadam, Sanyam Sharma and Jentz R. Method for Variable Position Exhaust Tuning Valve Diagnostic, US Patent number : 10844762
34. Dadam, S., Jentz, R., lenzen, T., and Meissner, H. ,Diagnostic Evaluation of Exhaust Gas Recirculation (EGR) System on Gasoline Electric Hybrid Vehicle 2020-01-0902 https://doi.org/10.4271/2020-01-0902
35. ZHU, D., PRITCHARD, E., DADAM, S.R. et al. Optimization of rule-based energy management strategies for hybrid vehicles using dynamic programming. Combustion Engines. 2021. https://doi.org/10.19206/CE-131967
36. Michiel J Van Nieuwstadt, Allen Lehmen, Douglas Raymond Martin, John Eric Rollinger, Sumanth Dadam, Rohit Bhat , *Gasoline particulate filter diagnostics* Patent number: 10323562
37. Robert Jentz, Tyler Lenzen, Sumanth Dadam, Herbert Meissner, Kent Hancock , *Method and system for exhaust gas recirculation system diagnostics* Patent number : 10632988
38. Robert Roy Jentz, Sanyam Sharma, Sumanth Dadam, *Heat exchanger for exhaust tuning systems* Patent number: 10436087
39. Exhaust gas heat recovery system with integrated Phase Change Material Heat Exchanger U.S. Patent No: 10961884
40. Sumanth Dadam, GPF Downstream Hose EGHR Diagnostic on Hybrids U.S. Patent number: 10928275
41. Snyder, K. and Ku, J., "Plug-in Hybrid Electric Vehicle Reengineering of a Conventional Sedan for EcoCAR2," SAE Technical Paper 2015-01-1235, 2015, https://doi.org/10.4271/2015-01-1235
42. Snyder, K. and Ku, J., "Advancement and Validation of a Plug-In Hybrid Electric Vehicle Plant Model," SAE Technical Paper 2016-01-1247, 2016, https://doi.org/10.4271/2016-01-1247
43. A. Rehman, S. Ur Rehman, M. Khan, M. Alazab and T. R. G, "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network using CNN and Attention-based GRU," in *IEEE Transactions on Network Science and Engineering*, doi: 10.1109/TNSE.2021.3059881.
44. Blevins, Deborah & Moriano, Pablo & Bridges, Robert & Verma, Miki & Iannacone, Michael & Hollifield, Samuel. (2021). Time-Based CAN Intrusion Detection Benchmark. 10.14722/autosec.2021.23013.
45. Plug-N-pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT(2020). 29th {USENIX} Security Symposium ({USENIX} Security 20)

Contact Information

Contact details for the main author should be included here. Details may include mailing address, email address, and/or telephone number (whichever is deemed appropriate).